AMENDMENTS TO THE CLAIMS

1. **(Currently Amended)** In a distributed computing environment, a method for managing an electronic record for compliance with network security policies of an organization, the method comprising:

creating an electronic tag that uniquely identifies the electronic record, the electronic tag being associated with a deletion prevention ~~specified~~ time period for compliance with the network security policies;

storing the ~~at least one~~ electronic tag in a central repository;

sending the electronic record ~~from the distributed computing environment~~ to a recipient computer; [[and]]

~~initiating the execution of scripting code upon the sending of the electronic record from the distributed computing environment to the recipient, the scripting code containing the procedures for handling the electronic record,~~

~~wherein the initiation of the execution of the scripting code prevents~~initiating execution of scripting code associated with the electronic tag to prevent the electronic record from being deleted before expiration of the deletion prevention time period associated with the electronic tag;

evaluating the electronic tag to determine if the electronic record is to be deleted based on expiration of the deletion prevention time period;

causing searching of the recipient computer for the electronic record; and

causing deletion of the electronic record from the recipient computer.

2. **(Currently Amended)** The method of claim 1, further comprising ~~deleting the electronic record and~~ selectively deleting the ~~at least one~~ electronic tag.

3. **(Original)** The method of claim 1, further comprising storing the electronic record.

4. **(Canceled)**

5. **(Previously Presented)** The method of claim 1, wherein the distributed computing environment comprises a computer having a registry and a user profile, and wherein creating the electronic tag comprises generating a reference code and creating the electronic tag at least in part as a function of at least one of the registry, the user profile, and the reference code.

6. **(Previously Presented)** The method of claim 5, wherein generating the reference code comprises reading the electronic record.

7. **(Previously Presented)** The method of claim 5, wherein the reference code comprises a classification code and an index code.

8. **(Previously Presented)** The method of claim 7, wherein the classification code is selected from a group comprising business email, personal email, intramail, bulletin board, minutemail, and purgemail.

9. **(Previously Presented)** The method of claim 7, wherein the index code identifies the contents of an electronic record and the recipient of the electronic record.

10. **(Currently Amended)** The method of claim 1, wherein creating the electronic tag comprises:

reading a stored electronic tag; and

generating an electronic tag in response to accessing an electronic record[[;]].

11. **(Previously Presented)** The method of claim 1, wherein the electronic record comprises an email message.

12. **(Previously Presented)** The method of claim 1, wherein sending the electronic record comprises:

reading the electronic tag; and

generating a new electronic tag at least in part as a function of the read electronic tag, a computer registry, a user profile, and a reference code.

13. **(Currently Amended)** In a distributed computing environment, an apparatus for managing an electronic record for compliance with network security policies, the apparatus comprising:

a computer system comprising at least one processor and at least one memory, the computer system being ~~adapted and arranged~~configured to

create an electronic tag that uniquely identifies the electronic record, the electronic tag being associated with a deletion prevention time period for compliance with the network security policies;

~~a central repository adapted to~~ store the electronic tag in a central repository storing a plurality of electronic tags each associated with one of a plurality of electronic records;

~~the distributed computing environment being adapted to~~ send the electronic record to a recipient computer; ~~and~~

~~scripting code, contained within the electronic tag, which is initiated and executed upon the sending of the electronic record from the distributed computing environment to the recipient, the scripting code containing the procedures for handling the electronic record,~~

~~wherein the initiation of the execution of the scripting code prevents the electronic record from being deleted before expiration of the deletion prevention time period associated with the electronic tag~~

evaluate the plurality of electronic tags stored in the central repository to identify an electronic tag for which the deletion prevention time period has elapsed;

cause searching of the recipient computer for an electronic record associated with the identified electronic tag; and

cause deletion of the electronic record associated with the identified electronic tag from the recipient computer.

14. **(Currently Amended)** The apparatus of claim 13, wherein the computer system is further adapted and arranged for purging the electronic record by deleting the electronic record associated with the identified electronic tag and selectively deleting the identified electronic tag.

15. **(Canceled)**

16. **(Original)** The apparatus of claim 13, wherein the distributing computing environment comprises a computer having a registry and a user profile, wherein the computer system is configured and arranged to: generate a reference code, wherein the electronic tag is generated at least in part as a function of at least one of the registry, the user profile, and the reference code.

17. **(Currently Amended)** In a distributed computing environment, an article of manufacture for managing an electronic record for compliance with network security policies, the article of manufacture comprising a computer-readable storage medium having a computer program embodied therein that causes the distributed computing environment to:

create an electronic tag that identifies the electronic record, the electronic tag being associated with a deletion prevention time period for compliance with the network security policies;

send the electronic record to a recipient computer;~~and~~

~~initiate scripting code upon the sending of the electronic record to a recipient, the scripting code containing the procedures for handling the electronic record;~~

~~wherein the initiation of the execution of the scripting code prevents the electronic record from being deleted before expiration of the deletion prevention time period associated with the electronic tag~~

evaluate the electronic tag to determine if the electronic record is to be deleted based on expiration of the deletion prevention time period;

cause searching of the recipient computer for the electronic record; and

causing deletion of the electronic record from the recipient computer.

18. **(Previously Presented)** The article of claim 17, wherein the computer program further causes the distributed computing environment to purge the electronic record by deleting the electronic record and selectively deleting the electronic tag.

19. **(Previously Presented)** The article of claim 17, wherein the computer program further causes the distributed computing environment to store the electronic record.

20. **(Canceled)**

21. **(Previously Presented)** The article of claim 17, wherein the distributed computing environment comprises a computer having a registry and a user profile, wherein the computer program further causes the distributed computing environment to generate a reference code, wherein the electronic tag is generated at least in part as a function of at least one of the registry, the user profile, and the reference code.

22. **(Previously Presented)** The article of claim 17, wherein the computer program further causes the distributed computing environment to:

read stored electronic tags; and

generate a further electronic tag in response to accessing an electronic record.

23. **(Currently Amended)** In a distributed computing environment, a method for managing an electronic record for compliance with network security policies of an organization, the method comprising:

creating an electronic tag that uniquely identifies the electronic record, the electronic tag being associated with a deletion prevention ~~specified~~ time period for compliance with the network security policies;

storing the ~~at least one~~ electronic tag in a central repository storing a plurality of electronic tags each associated with one of a plurality of electronic records;

sending the electronic record to a recipient computer; and

~~initiating the execution of scripting code upon the sending of the electronic record,~~

~~the scripting code containing the procedures for handling the electronic record,~~

~~wherein the initiation of the execution of the scripting code prevents the electronic record from being deleted before expiration of the deletion prevention time period associated with the electronic tag; and~~

~~wherein the distributed computing environment automatically monitors compliance with the network security policies as a function of the electronic tag~~

evaluating the plurality of electronic tags stored in the central repository to identify one or more electronic records to be deleted based on expiration of the deletion prevention time period;

evaluating a user profile of a user associated with the one or more electronic records to be deleted to determine a deletion privilege of the user;

according to the deletion privilege perform at least one of

deleting the electronic record to be deleted and the electronic tag associated therewith stored in the central repository; and

deleting the electronic record to be deleted without deleting the electronic tag associated therewith stored in the central repository.

24-26. **(Canceled)**

27. **(New)** A computing device operably coupled to a network comprising:

means for creating an electronic tag that uniquely identifies the electronic record, the electronic tag being associated with a deletion prevention time period for compliance with the network security policies;

means for storing the electronic tag in a central repository storing a plurality of electronic tags each associated with an electronic record;

means for sending the electronic record to a recipient computer

means for evaluating the plurality of electronic tags stored in the central repository to identify one or more electronic records to be deleted based on expiration of the deletion prevention time period;

means for causing searching of the recipient computer for the electronic records to be deleted; and

means for causing deletion of the electronic records to be deleted from the recipient computer.